Methods for Preserving Audiovisual Data

Cooperatively Utilizing Digital Fingerprints & Watermarks

W3C Video on the Web Workshop / December 13, 2007

Michael Wise
Group Technical Advisor, Platform R&D
Turner Broadcasting System, Inc.
Michael.Wise@Turner.com

Copyright 2007, Turner Broadcasting System, Inc.

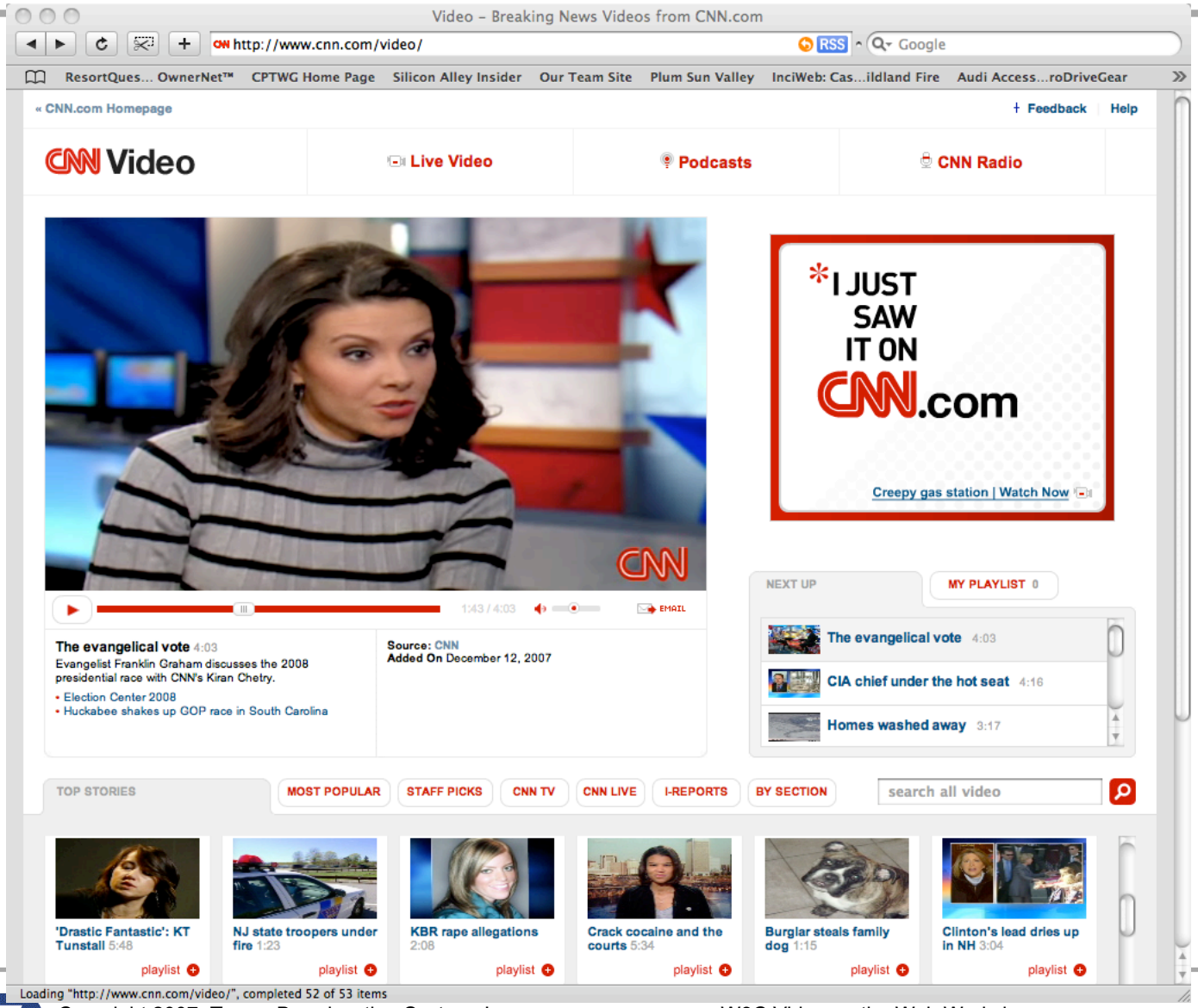
Time Warner Inc. 2004. All trademarks and service marks incorporated herein are owned by Time Warner Inc. and/or one of its affiliated companies.

Overview

- Despite the proliferation of video on the Web, the availability of quality, consistent metadata remains elusive
  - Standards, related implementation issues cause inconsistency
  - Syndication and the repurposing of traditional linear content feeds for the Web complicates metadata survivability
  - Transcoding, transcrypting, and substitution of container formats can all affect metadata integrity and survivability
  - A significant amount of content is (re)published by publishers unaffiliated with content owners or distributors causes metadata unpredictability
- Lack of quality metadata has several consequences
  - Suboptimal search results
  - Complicates enforcement of usage rights
  - Affects ability to reliably measure and monetize content usage
- Digital watermarking and fingerprinting can help maintain metadata integrity through production, distribution, and consumption chains

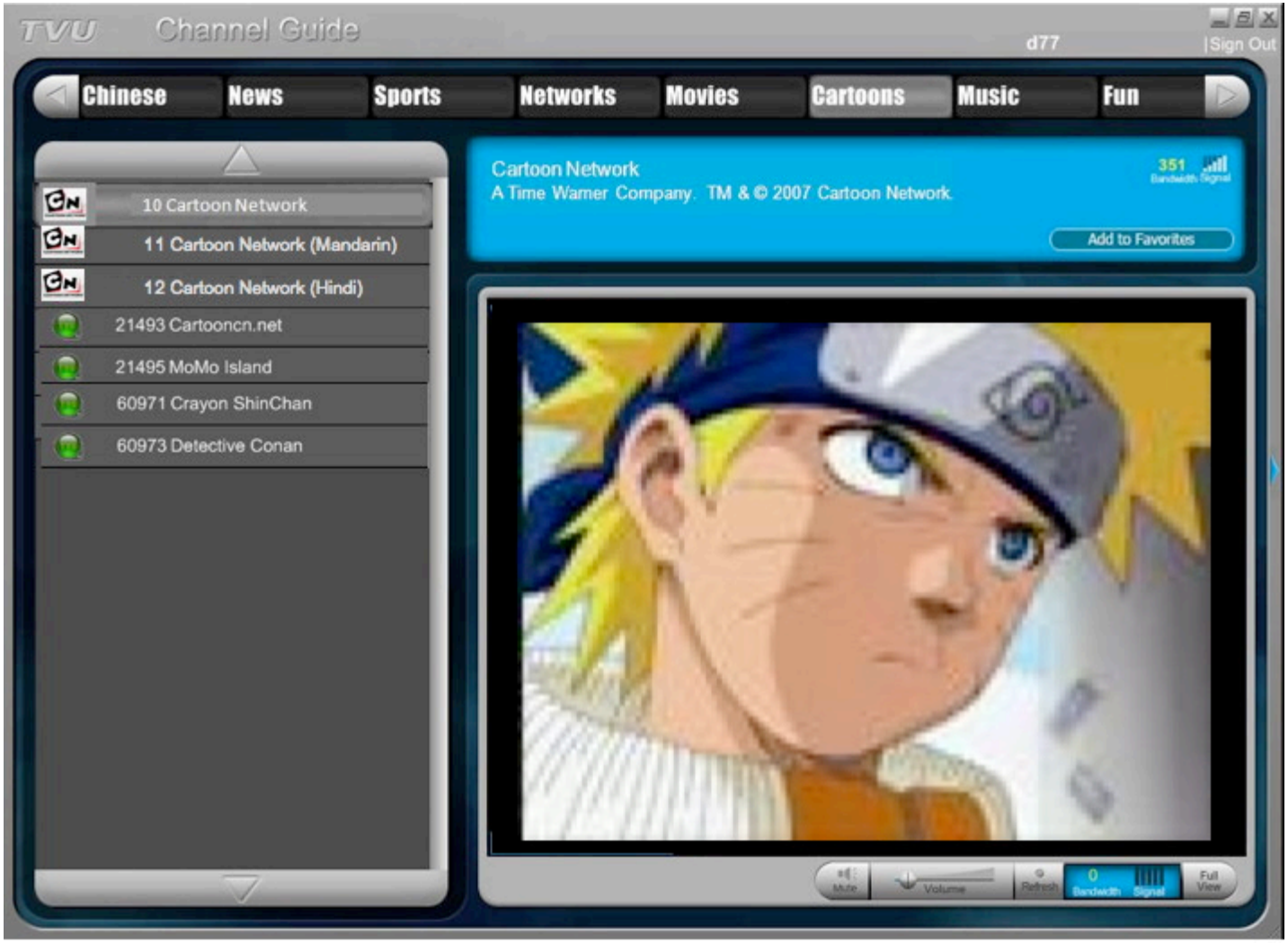
Copyright 2007, Turner Broadcasting System, Inc.

CNN.com Hosted Video: Rich, Accurate Metadata



Copyright 2007, Turner Broadcasting System, Inc.

Syndicated Linear Video: Less Metadata



Copyright 2007, Turner Broadcasting System, Inc.

User Re-encoded Linear Content on the Web: Potentially Unpredictable Metadata

Copyright 2007, Turner Broadcasting System, Inc.

Digital Watermarks and Fingerprints Defined

- Digital Watermarking technologies enable the addition of a hidden message to an audiovisual file
  - Current digital watermarking technologies have the ability to survive common transformations such as re-encoding, sub–sampling, and cropping of the original media files
  - There are tradeoffs and relationships between watermark transparency, recoverability, survivability, and payload size
  - Practical payload sizes are typically 3-10 bits/second
  - Many vendors

- Digital Fingerprinting is the calculation of a unique “fingerprint” of a segment of content
  - A segment is identified by calculating a fingerprint of the content and performing a comparison against a database of known fingerprints
  - Many vendors

Copyright 2007, Turner Broadcasting System, Inc.

Possible Applications of Digital Watermarks and Fingerprints

- Possible uses of these technologies are many. Examples include:
  - Facilitation of usage measurement through the embedding of a unique ID analogous to a UPC code
  - Assistance in the enforcement of various usage rules through the embedding of usage flags
  - Identifying when and where an asset transited various distribution points through the embedding of forensic watermarks
- Improved monetization opportunities could be possible

Copyright 2007, Turner Broadcasting System, Inc.

Challenges in Broadly Implementing Digital Watermark Technologies

- Effective digital watermark payload sizes are small relative to ideal metadata payloads
- Unpredictable results occur when multiple watermark technologies are applied to a content segment
- Fingerprinting can augment efforts to identify content, but
  - Can be computationally more expensive than watermark detection
  - Doesn't enable certain metadata to be "self identifying"

Technical constraints will likely require industry cooperation to meaningfully leverage digital watermark and fingerprint technologies to preserve metadata

Copyright 2007, Turner Broadcasting System, Inc.